UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/713,771	11/14/2003	Isaac J. Mosgrove	612-65525	8766

			EXAMINER
24197	7590	09/08/2005	YANG, CLARA I

KLARQUIST SPARKMAN, LLP
121 SW SALMON STREET
SUITE 1600
PORTLAND, OR 97204

ART UNIT	PAPER NUMBER
2635	

DATE MAILED: 09/08/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on <u>05 July 2005</u>.
2a) ☒ This action is **FINAL**.   2b) ☐ This action is non-final.
3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) *1-26 and 32* is/are pending in the application.
   4a) Of the above claim(s) _____ is/are withdrawn from consideration.
5) ☒ Claim(s) *15,16 and 21-26* is/are allowed.
6) ☒ Claim(s) *1-14,17-20 and 32* is/are rejected.
7) ☐ Claim(s) _____ is/are objected to.
8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) ☐ The specification is objected to by the Examiner.
10) ☒ The drawing(s) filed on *14 November 2003* is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
   Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
   Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All   b) ☐ Some * c) ☐ None of:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____.
      3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
   * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
   Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413)
   Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

1.   Applicant's arguments filed on 5 July 2005 with respect to claims 1-6 have been

considered but are moot in view of the new ground(s) of rejection.

2.   Applicant's arguments filed on 5 July 2005 have been fully considered but they are not

persuasive.

On page 12, the applicant argues that Wunderlich (US 6,611,232) does not teach an

electronic access device as recited in claim 32. The applicant states, "The Examiner erroneously

suggests that the IR transmitter of Wunderlich is an electronic access device. As mentioned

above [in the arguments regarding claims 1 and 2], the IR transmitters are located in a lock box

unit, which is assigned to a particular vehicle and not to a particular user as recited in claim 32."

In the arguments regarding claims 1 and 2, the applicant assumes that the examiner is referring

to transmitter 280 disclosed in Wunderlich (see page 11). However, the applicant's assumption

is incorrect, because the examiner understands that transmitter 280 transmits a spread spectrum

response signal R to receiving stations 150 (see Col. 4, lines 37-44). Wunderlich's IR transmitter

for communicating with identification device 430 is a different device from transmitter 280.

In Col. 6, lines 1-17, Wunderlich teaches that lock box unit 110 contains an identification

device 430 (see Fig. 4), which may be a variety of known devices such as an infrared (IR) reader

device (see Col. 6, lines 2-5). In other words, identification device 430 can be an IR receiver. Per

Wunderlich, identification device 430 is used to "identify the person unlocking key box 210 by

recording an identification code for the person when the key box is accessed", wherein

identification device 430 "may obtain the identification code of the user by...reading an IR

input" (see Col. 6, lines 5-10). In other words, identification device 430 receives a person's

identification code that is transmitted by an IR transmitting device, which must have a memory for storing the person's identification code. Wunderlich adds that the received identification information is used to track which sales people accesses particular vehicles and that identification device 430 serves as a security device that prevents access to key box 210 to particular authorized persons (see Col. 6, lines 13-17). Thus Wunderlich does teach an electronic access device (such as an IR transmitting device) as recited in claim 32, and examiner maintains the 35 USC 102(e) rejection of claim 32.

On pages 14-15, the applicant argues that the combination of Greenman, Pires, and Danler fails to teach the key management system called for in claim 7, specifically an access device that has a memory that is updated with at least a key tag identifier when the key container is successfully access and the key set is removed from a key set storage area. As support for the argument, the applicant states that Danler fails to teach the following: (1) a key set (see page 14) and (2) updating an electronic access device's memory when the key container is successfully accessed and the key set is removed from the key set storage area (see page 15). The applicant adds that Greenman and Pires fail to overcome the deficiencies of Danler. The examiner respectfully disagrees. First of all, Pires teaches a key storage system 1 comprising: (a) at least one key set formed by key 4, wire 3, and key tag 2 (herein after "key tag 2"), wherein key tag 2 has electronic memory device 53 that stores an electronically readable identifier and provides an electrical contact portion (see Col. 4, lines 56-57 and Col. 5, lines 27-64); and (b) housing 17 or key container having a storage area that includes a plurality of stations 6 for detecting key tag 2 when key tag 2 is inserted properly into receptacle 7 (see Col. 4. lines 20-24; Col. 5, lines 27-37; and Col. 7, lines 15-18). Per Pires, each station 6 has a plunger 29 and solenoid 23 (i.e., electronic lock) for preventing removal of a key set by an unauthorized person,

and the same arrangement is used for securing housing 17 (see Col. 5, lines 65-67 and Col. 6, lines 1-10). Pires also discloses that station 6 communicates with key tag 2 when the electrical contact portion of key tag 2's memory device 53 is placed to complete an electrical circuit of station 6 (see Col. 5, lines 27-37 and Col. 8, lines 22-43), as called for in claim 17. Furthermore, system 1 of Pires maintains a database on (1) when housing 17 is accessed, (2) the identity of a key tag 2 that is removed and the time of removal, and (3) the identity of a key tag 2 that is returned and the time of return (see Col. 1, lines 48-50; Col. 5, lines 33-37; and Col. 9, lines 31-41). In other words, system 1 updates its database with at least the identifier of a key tag 2 when housing 17 is successfully accessed and key tag 2 is removed from station 6. Though Pires is silent on transferring the contents of system 1's database (which includes key tag 2's identifier and the time when key tag 2 has been removed), thereby updating a portable electronic access device, Danler teaches electronic key 14 (i.e., access device) downloading and storing lock box 12's access log, which includes the date and time of each access (see Col. 21, lines 55-64). Consequently, Greenman, as modified by Pires and Danler, teaches all the limitations of claim 7, and the 35 USC 103(a) rejection of claim 7 and its dependent claims is maintained.

Regarding the applicant's argument concerning claim 11 (see page 15), system 1 of Pires maintains a database on (1) when housing 17 is accessed, (2) the identity of a key tag 2 that is removed and the time of removal, and (3) the identity of a key tag 2 that is returned and the time of return (see Col. 1, lines 48-50; Col. 5, lines 33-37; and Col. 9, lines 31-41). Pires, however, is silent on updating a portable electronic access device by transferring the contents of system 1's database (which includes the identity of a key tag 2 that is returned and the time of return) to the portable electronic access device. Danler, on the other hand, teaches electronic key 14

(i.e., access device) downloading and storing lock box 12's access log, which includes the date and time of each access (see Col. 21, lines 55-64). Consequently, Greenman, as modified by Pires and Danler, teaches all the limitations of claim 11, and the 35 USC 103(a) rejection of claim 11 is maintained.

Regarding claim 18, the applicant argues on page 16 that "Greenman makes no mention of a challenge response exchange between the lock 101 and a PDA or cell phone." However, Danler discloses that electronic key 14 and lock box 12 participate in a challenge-response exchange when a user attempts to access lock box 12 (see Col. 14, lines 37-44) as indicated by the examiner on page 12 of the Office Action mailed on 30 March 2005. Consequently, Greenman, as modified by Pires and Danler, teaches all the limitations of claim 18, and the 35 USC 103(a) rejection of claim 11 is maintained.

Regarding claim 14, as explained above, the combination of Greenman, Pires, and Danler teaches all the limitations of claim 7; thus the 35 USC 103(a) rejection of claim 14 is maintained.

Allowable Subject Matter

1.   Claims 15, 16, and 21-26 are allowed.

Claim Rejections-35 USC § 102

2.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States

only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3.   Claim 32 is rejected under 35 U.S.C. 102(e) as being anticipated by Wunderlich et al. (US 6,611,232).

Referring to claim 32, Wunderlich's key management system, as shown in Figs. 1, 2, and 5, comprises: (a) vehicle keys 215 for a plurality of vehicles on a vehicle lot (see Col. 3, lines 11-12); (b) a lock box unit 110 attached to each vehicle, wherein each lock box unit 110 has a key box 210 for storing a vehicle key (see Col. 3, lines 12-14 and Col. 4, lines 25-28); (c) an IR transmitter (i.e., electronic access device) assigned to a user for unlocking lock box unit 110 if authorized (see Col. 3, lines 39-44 and Col. 6, lines 1-17); and (d) a database stored on central computer 170 and containing the identity of each vehicle on the lot, the unique address of each vehicle's lock box unit 110, and the identification of the users (see Col. 5, lines 8-17 and Col. 6, lines 11-17 and 26-31). Because Wunderlich teaches that lock box unit 110 is able to prevent access to particular authorized persons based on a received identification (see Col. 6, lines 15-17), the identification of the users also functions as a user's access privilege; thus Wunderlich's database stored in central computer 170 further includes access privileges of the users. Wunderlich's IR transmitters must be programmable in order to accept a user's identification (i.e., information from the database) and to enable a user to access a lock box unit by using the IR transmitter (see Col. 6, lines 8-10 and 15-17).

Claim Rejections-35 USC § 103

4.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and

the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5.   This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

6.   Claims 1-5 are rejected under 35 U.S.C. 103(a) as being unpatentable over Greenman (US 2003/0179075) in view of Danler (US 5,280,518).

Referring to claim 1, Greenman teaches a property access system, as shown in Figs. 1a and 2, comprising: (a) lock 101 (i.e., a key container) located proximal to a vehicle having a key compartment 105 for storing vehicle key 121, an electronic lock for securing key compartment 105, and a microcontroller 119 for storing authorized access codes and controlling the electronic lock (see Sections [0026], [0028], [0031], and [0038]); and (b) an electronic key, such as a personal digital assistant (PDA) or cell phone, for communicating with lock 101 via IR or RF, wherein the electronic key has a memory for storing access codes (see Sections [0028], [0037] and [0061]). Greenman discloses that microcontroller 119 opens the electronic lock and (c) records the access code and time of entry (i.e., access events) when a received access code matches an encrypted access code (see Sections [0038] and [0069]); thus microcontroller 119 must have a memory. Greenman, however, fails to teach storing access events in the PDA or cell phone during an access for later uploading to a central computer.

In an analogous art, Danler teaches a key management system, as shown in Fig. 1, comprising: (a) key 20; (b) lock box 12 having a key container 64 secured by locking solenoid 66 (see Col. 4, lines 39-42 and Col. 6, lines 5-10); and (c) electronic key 14 (i.e., portable electronic access device) for accessing key container 64, wherein electronic key 14 has a key memory 148 that is updated with lock box 12's identifier when key container 64 is successfully accessed (see Col. 16, lines 20-28). In other words, electronic key 14 stores access events during an access. Per Danler, the contents stored in electronic key 14 are then uploaded to central computer 18 (see Col. 13, lines 49-51 and Col. 14, lines 15-19).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Greenman's system as taught by Danler because a PDA or cell phone that stores access events enables system 1 to use the PDA or cell phone for audits (see Danler, Col. 2, lines 37-42).

Regarding claims 2-5, Greenman teaches in Sections [0011], [0037], [0061], and [0067], that lock 101 and an electronic key communicates via IR (as called for in claim 2) or RF (as called for in claim 3) and that the electronic key is a pocket-sized computer (i.e., a PDA) or a smart cell phone (as called from in claims 4 and 5 respectively). Greenman's PDS and smart cell phone must be open architecture devices in order to control Greenman's lock 101.

7.   Claim 6 is rejected under 35 U.S.C. 103(a) as being unpatentable over Greenman (US 2003/0179075) in view of Danler (US 5,280,518) as applied to claim 1 above, and further in view of Pires (US 6,131,808).

Regarding claim 6, Greenman, as modified by Danler, omits teaching a key tag associated with the vehicle key, wherein the key tag has an electronically stored identifier and being detectible by the lock box when placed in the key storage area.

In an analogous art, Pires teaches a key storage system 1 comprising: (a) at least one key set formed by key 4, wire 3, and key tag 2 (i.e., key tag), wherein key tag 2 has electronic memory device 53 that stores an electronically readable identifier and provides an electrical contact portion (see Col. 4, lines 56 - 57 and Col. 5, lines 27 - 64); and (b) housing 17 or key container having a storage area that includes a plurality of stations 6 for detecting key tag 2 when key tag 2 is inserted properly into receptacle 7 (see Col. 4. lines 20 - 24; Col. 5, lines 27 - 37; and Col. 7, lines 15 - 18). Per Pires, each station 6 has a plunger 29 and solenoid 23 (i.e., electronic lock) for preventing removal of a key set by an unauthorized person, and the same arrangement is used for securing housing 17 (see Col. 5, lines 65 - 67 and Col. 6, lines 1 - 10). Pires also discloses that station 6 communicates with key tag 2 when the electrical contact portion of key tag 2's memory device 53 is placed to complete an electrical circuit of station 6 (see Col. 5, lines 27 - 37 and Col. 8, lines 22 - 43). Furthermore, system 1 of Pires maintains a database on when housing 17 is accessed, the identity of a key tag 2 that is removed and the time of removal, and the identity of a key tag 2 that is returned and the time of return (see Col. 1, lines 48 - 50; Col. 5, lines 33 - 37; and Col. 9, lines 31 - 41). In other words, system 1 updates its database with at least the identifier of a key tag 2 when housing 17 is successfully accessed and key tag 2 is removed from station 6.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the lock box system of Greenman and Danler per the teachings of Pires since a key having a key tag and a key receptacle that detects and communicates with the key tag enable an automobile dealership to ensure only authorized removal of keys and to determine who has removed a key, which key has been removed, and when the key has been

removed (see Pires, Col. 1, lines 15 - 21 and 39 -41), thereby reducing the likelihood of lost keys and vehicle theft.

8.   Claims 7-13 and 17-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Greenman (US 2003/0179075) in view of Pires (US 6,131,808) and Danler (US 5,280,518).

Referring to claims 7-11, 17, and 18, Greenman discloses a vehicle key access system, as explained above in the rejection of claim 1. Regarding claim 7, Greenman's system, as shown in Fig. 1, comprises: (a) key 121 (see Section [0026]); (b) lock 101 (i.e., a key container) that is located on the vehicle and having key compartment 105 secured by an electronic lock (see Sections [0026] and [0031]); and (c) an open architecture PDA or cell phone, as explained above in the rejection of claim 1, having a memory that stores at least one access code (see Sections [0011] and [0061]). Greenman, however, omits teaching the following: (1) key 121 is associated with a key tag having an electronically readable identifier stored thereon and an electronic contact portion; (2) lock 101 detects a key tag when the key set formed by key 121 and the key tag are properly stored in key compartment 105; and (3) the memory of the PDA or cell phone is updated with at least the key tag's identifier when lock 101 is successfully accessed and the key set is removed from key compartment 105. Consequently, Greenman also fails to teach that: (4) lock 101 has a memory for storing at least the key tag's identifier (as called for in claim 8); and (5) lock 101 communicates with the key tag when the electrical contact portion of the key tag is placed in electrical contact with the key container (as called for in claim 17). In addition, Greenman is silent on: (6) lock 101's memory including a list that identifies an unauthorized access device or an unauthorized user (as called for in claim 9); (7) a PDA's or cell phone's memory storing the approximate time when the key tag removed from key compartment 105 (as called for in claim 10) and when the key was returned to key compartment 105 (as called for

in claim 11); and (8) lock 101 and a PDA or cell phone participating in a challenge-response exchange when a user attempts to access lock 101 (as called for in claim 18).

In an analogous art, as called for in claim 7, Pires teaches a key storage system 1 comprising: (a) at least one key set formed by key 4, wire 3, and key tag 2 (herein after "key tag 2"), wherein key tag 2 has electronic memory device 53 that stores an electronically readable identifier and provides an electrical contact portion (see Col. 4, lines 56-57 and Col. 5, lines 27-64); and (b) housing 17 or key container having a storage area that includes a plurality of stations 6 for detecting key tag 2 when key tag 2 is inserted properly into receptacle 7 (see Col. 4. lines 20-24; Col. 5, lines 27-37; and Col. 7, lines 15-18). Per Pires, each station 6 has a plunger 29 and solenoid 23 (i.e., electronic lock) for preventing removal of a key set by an unauthorized person, and the same arrangement is used for securing housing 17 (see Col. 5, lines 65-67 and Col. 6, lines 1-10). Pires also discloses that station 6 communicates with key tag 2 when the electrical contact portion of key tag 2's memory device 53 is placed to complete an electrical circuit of station 6 (see Col. 5, lines 27-37 and Col. 8, lines 22-43), as called for in claim 17. Furthermore, system 1 of Pires maintains a database on (1) when housing 17 is accessed, (2) the identity of a key tag 2 that is removed and the time of removal, and (3) the identity of a key tag 2 that is returned and the time of return (see Col. 1, lines 48-50; Col. 5, lines 33-37; and Col. 9, lines 31-41), as called for in claim 8. In other words, system 1 updates its database with at least the identifier of a key tag 2 when housing 17 is successfully accessed and key tag 2 is removed from station 6. Pires, however, is silent on updating a portable electronic access device with key tag 2's identifier when key tag 2 has been removed (as called for in claim 7). Pires also fails to teach the limitations of claims 9-11 and 18.

In another analogous art, Danler teaches a key management system, as shown in Fig. 1, comprising: (a) key 20; (b) lock box 12 having a key container 64 secured by locking solenoid 66 (see Col. 4, lines 39-42 and Col. 6, lines 5-10); and (c) electronic key 14 (i.e., portable electronic access device) for accessing key container 64, wherein electronic key 14 has a key memory 148 that is updated with lock box 12's identifier when key container 64 is successfully accessed (see Col. 16, lines 20-28), as called for in claim 7. Danler's lock box 12 also includes a memory that stores a list of unauthorized electronic keys/access devices (see Col. 10, lines 65-58 and Col. 11, lines 1-8), as called for in claim 9. In addition, Danler teaches that electronic key 14 is able to store lock box 12's access log, which includes the date and time of each access (see Col. 21, lines 55-64). Here it is understood that lock box 12 must be accessed in order to return the key. Thus by downloading lock box 12's access log, Danler's electronic key 14 stores the approximate times when electronic key 14 accessed lock box 12 to retrieve and return the key, as called for in claims 10 and 11. Finally, Danler discloses that electronic key 14 and lock box 12 participate in a challenge-response exchange when a user attempts to access lock box 12 (see Col. 14, lines 37-44), as called for in claim 18.

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the key and key receptacle of Greenman as taught by Pires because a key having a key tag 2 and a lock 101 that detects and communicates with key tag 2 enable an automobile dealer to ensure only authorized removal of keys and to determine who has removed a key, which key has been removed, and when the key has been removed (see Pires, Col. 1, lines 15-21 and 39 -41), thereby reducing the likelihood of lost keys and vehicle theft. In addition, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the system of Greenman and Pires as taught by Danler

because (1) a challenge-response exchange between lock 101 and a PDA or cell phone enhances security (see Danler, Col. 14, lines 22-25) and (2) a lock 101 that updates a PDA or cell phone with at least the identifier of key tag 2 when key tag 2 is removed from the key receptacle and when the PDA or cell phone successfully removed and returned the key enables system 1 to use the PDA or cell phone for audits (see Danler, Col. 2, lines 37-42).

Regarding claim 12, Greenman suggests setting up a central computer 420 within central facility 419 for administering the system by allowing an authorized user (or administrator) to generate access codes and usage reports for each user or user groups (see Sections [0029], [0033], [0034], [0052], [0072] and [0073]). Because central computer 420 is able to generate usage reports (i.e., track a user's access activity), central facility 419 must have a database.

Regarding claim 13, Greenman teaches that the access codes generated by central computer 420 are valid for particular time periods (see Sections [0030], [0033], [0035], [0059], [0064], and [0072]). Thus, if a user fails to access lock 101 within the specified time period, causing the access code to expire, the user must use central computer 420 to generate a new access code for a new time period (i.e., reestablish his or her expired access privileges).

Regarding claim 19, Greenman's PDA or cell phone stores a user's access codes that are set to expire periodically (see Sections [0011], [0030], [0061], and [0068]).

Regarding claim 20, Greenman's lock 101 has a controller 119 for generating valid access codes that are used to determine whether or not to grant access to a user by comparing the user's access code with those stored in controller 119 (see Sections [0031], [0038], [0053]-[0061], and [0064]). Controller 119 must temporarily store each generated access code in order to determine if a user's access code is valid.

9.   Claim 14 is rejected under 35 U.S.C. 103(a) as being unpatentable over Greenman (US

2003/0179075) in view of Pires (US 6,131,808) and Danler (US 5,280,518) as applied to claim 7

above, and further in view of Maloney (US 5,801,628).

As explained above in the rejection of claim 19, Greenman, Pires, and Danler teach a

user using a PDA or cell phone to communicate the user's access code but fail to suggest the

user using the PDA or cell phone to select and communicate a code indicating the purpose of

the access.

In an analogous art, Maloney teaches a system comprising: (a) a key set having a vehicle

key 202 and a identification assembly 182 (hereinafter referred to as "key tag 182"), wherein key

tag 182 has an electronically readable identifier stored electronic device 194, which has an

electrical contact portion (see Figs. 7 and 12-15; Col. 1, lines 57-62; Col. 12, lines 50-54; Col. 13,

lines 3-8 and 27-45); (b) a key storage unit 52 or key container that is secured electrically-

actuated lock mechanism 218 and detects they key set when the key set is stored in drawer 98

(see Figs. 1 and 4; Col. 11, lines 22-45; Col. 13, lines 59-67; and Col. 14, lines 1-10 and 39-51); and

(c) remote controller 54 having a memory that is updated with at least the identifier of key tag

182 when it is removed from drawer 98 (see Col. 7, lines 14-29). Maloney imparts that a user

wishing to remove a key set uses remote controller 54 to enter information related to the

removal of the key set, such as reason for the removal of the key set and/or work order number

(see Col. 22, lines 57-67 and Col. 23, lines 1-5). Because Maloney teaches that the work order

number identifies the task to be performed, work order numbers are understood to form a

predetermined group of codes corresponding to the purpose of the access.

Therefore, it would have been obvious to one having ordinary skill in the art at the time

the invention was made to modify the PDA or cell phone of Greenman, Pires, and Danler as

taught by Maloney because a PDA of cell phone that is used to provide a predetermined code corresponding to the purpose of the removal enables the system to provide a more detailed record of a key set, thereby reducing potential for abuse (see Maloney, Col. 2, lines 4-25).

Conclusion

10.   **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

⌘⌘⌘

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Clara Yang whose telephone number is (571) 272-3062. The examiner can normally be reached on 8:30 AM - 7:00 PM, Monday - Thursday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Michael Horabik can be reached on (571) 272-3068. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

CY
1 September 2005

BRIAN ZIMMERMAN
PRIMARY EXAMINER